PATENT ABSTRACTS OF JAPAN

(11)Publication number : 05-347616
(43)Date of publication of application : 27.12.1993

(51)Int.Cl. H04L 9/06
H04L 9/14
H04L 12/28

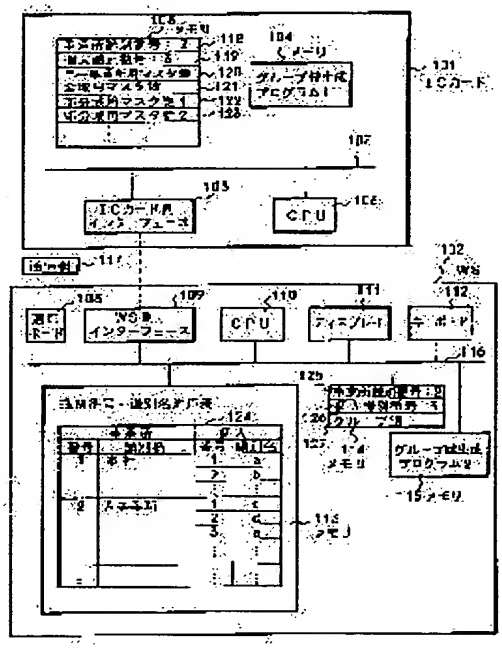
(21)Application number : 04-154733
(22)Date of filing : 15.06.1992

(71)Applicant : HITACHI LTD
HITACHI CHUBU SOFTWARE LTD

(72)Inventor : TAKARAGI KAZUO
SUZAKI SEIICHI
MATSUMOTO HIROSHI
NAKAMURA TSUTOMU

(54) GROUP CIPHERING COMMUNICATION METHOD AND GROUP CIPHERING COMMUNICATION SYSTEM

(57)Abstract:
PURPOSE: To attain group ciphering communication from one optional terminal to lots of optional terminals among plural terminals while the security is ensured.
CONSTITUTION: Plural secret numerals called as a master key in common to a prescribed partial set in an IC card 101 are stored in a memory 103 of the IC card, the IC card is inserted to a terminal to which communication is started at first to generate communication destination information is generated and sent to other terminal via a communication network 117. Moreover, based on communication destination information, one is selected from plural master keys and a group key is generated by using the selected master key and a communication message is ciphered or decoded by using the generated group key. A terminal being a communication destination receives communication destination information and selects one from the plural master keys based on the communication destination information and the group key is generated by using the selected master key and ciphering/decoding of the communication message is implemented by using the generated group key.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（Ａ）**　(11)特許出願公開番号

特開平5－347616

(43)公開日　平成５年(1993)12月27日

(51)Int.Cl.[5]	識別記号	庁内整理番号	Ｆ Ｉ	技術表示箇所
Ｈ０４Ｌ　9/06				
9/14				
12/28				
		7117－5K	Ｈ０４Ｌ　9/ 02	Ｚ
		8529－5K	11/ 00　３１０	Ｚ

審査請求　未請求　請求項の数14(全 16 頁)

(21)出願番号　特願平4－154733

(22)出願日　平成４年(1992)６月15日

(71)出願人　000005108
株式会社日立製作所
東京都千代田区神田駿河台四丁目６番地

(71)出願人　000233457
日立中部ソフトウェア株式会社
愛知県名古屋市中区栄３丁目10番22号

(72)発明者　宝木　和夫
神奈川県川崎市麻生区王禅寺1099番地　株式会社日立製作所システム開発研究所内

(72)発明者　洲崎　誠一
神奈川県川崎市麻生区王禅寺1099番地　株式会社日立製作所システム開発研究所内

(74)代理人　弁理士　小川　勝男

最終頁に続く

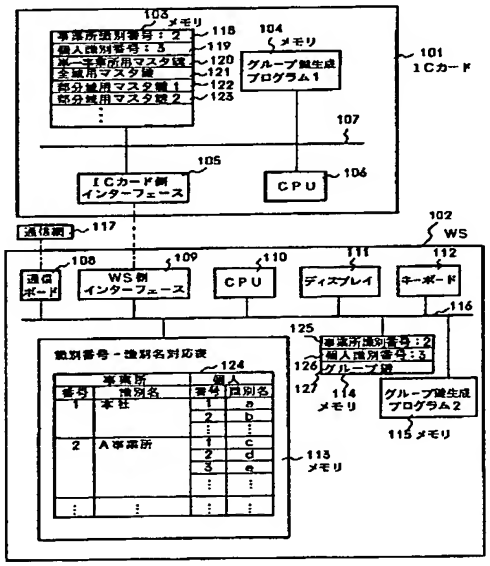
(54)【発明の名称】　グループ暗号通信方法およびグループ暗号通信システム

(57)【要約】　(修正有)

【目的】セキュリティ上の安全を確保しつつ、複数端末間で任意の１つの端末から任意の多数の端末へとグループ暗号通信ができるようにする。

【構成】ＩＣカード１０１に、ＩＣカードの所定の部分集合において共通であるマスタ鍵と呼ばれる秘密数値をメモリ１０３に複数個格納し、最初に通信を開始する端末にＩＣカードを差し込み、通信宛先情報を生成し通信網１１７を介し他の端末に送出する。また通信宛先情報に基づいて複数のマスタ鍵から１つを選択し、選択したマスタ鍵を用いてグループ鍵を生成し、生成したグループ鍵を用いて通信メッセージの暗号化および復号化を行う。通信宛先である端末においては、通信宛先情報を受け取り、該通信宛先情報に基づいて複数のマスタ鍵から１つを選択し、選択したマスタ鍵を用いてグループ鍵を生成し、生成したグループ鍵を用いて通信メッセージの暗号化および復号化を行う。

図１



【特許請求の範囲】

【請求項１】複数のＩＣカードと、ＩＣカードの入出力インターフェースを有する複数の通信端末と、それらの通信端末を結ぶ通信網とを備えた通信システムに適用するグループ暗号通信方法であって、

前記ＩＣカードには、各ＩＣカードを特定する個別の数値、およびＩＣカードの所定の部分集合において共通であるマスタ鍵と呼ばれる秘密数値が複数個格納されており、

最初に通信を開始する端末においては、通信を行うべき相手先を特定する通信宛先情報を生成して、他の端末に送出するとともに、該通信宛先情報に基づいて自端末に差し込まれているＩＣカードに格納されている前記複数のマスタ鍵から１つを選択し、選択したマスタ鍵を用いてグループ鍵を生成し、生成したグループ鍵を用いて通信メッセージの暗号化および復合化を行って、通信メッセージを授受し、

通信宛先である端末においては、前記通信宛先情報を受け取り、該通信宛先情報に基づいて自端末に差し込まれているＩＣカードに格納されている前記複数のマスタ鍵から１つを選択し、選択したマスタ鍵を用いてグループ鍵を生成し、生成したグループ鍵を用いて通信メッセージの暗号化および復合化を行って、通信メッセージを授受することを特徴とするグループ暗号通信方法。

【請求項２】前記通信宛先情報は、通信を行うべき相手先を特定する情報と任意に選択された数値情報とからなり、かつ前記グループ鍵は、前記選択したマスタ鍵および前記通信宛先情報を用いて生成される請求項１に記載のグループ暗号通信方法。

【請求項３】前記グループ鍵は、ハッシュ関数を用いた計算によって生成される請求項１または２に記載のグループ暗号通信方法。

【請求項４】前記ＩＣカードに格納されている個別の数値を用いて前記通信宛先情報を検査し、これにより該通信宛先情報が該ＩＣカードの個別の数値を指定しているか否かを判定する請求項１ないし３に記載のグループ暗号通信方法。

【請求項５】前記通信宛先情報に基づいて前記複数のマスタ鍵から１つを選択し選択したマスタ鍵を用いてグループ鍵を生成する処理が、ＩＣカード内部で実行される請求項１ないし４に記載のグループ暗号通信方法。

【請求項６】前記ＩＣカードにはさらに、暗号関数およびＩＣカードごとに異なる個別鍵と呼ばれる秘密数値が格納されており、該ＩＣカードのマスタ鍵の更新は、マスタ鍵を個別鍵で暗号化したマスタ鍵暗号文を外部からＩＣカードに入力し、該マスタ鍵暗号文を個別鍵と暗号関数を用いて復号化し、その結果を前記マスタ鍵が書かれていた記憶領域上に上書きすることにより行う請求項１ないし５に記載のグループ暗号通信方法。

【請求項７】前記ＩＣカードにはさらに、暗号関数およびＩＣカードごとに異なる第１，第２，…の個別鍵と呼ばれる秘密数値が複数個格納されており、該ＩＣカードのマスタ鍵の更新は、マスタ鍵を第１の個別鍵で暗号化したマスタ鍵分割暗号文を外部からＩＣカードに入力し、マスタ鍵を第２の個別鍵で暗号化したマスタ鍵分割暗号文を外部からＩＣカードに入力し、…、このようにＩＣカードに入力された複数のマスタ鍵分割暗号文を前記第１，第２，…の個別鍵と暗号関数を用いてそれぞれ復号化し、その結果に所定の演算を施した結果を前記マスタ鍵が書かれていた記憶領域上に上書きすることにより行う請求項１ないし５に記載のグループ暗号通信方法。

【請求項８】複数のＩＣカードと、ＩＣカードの入出力インターフェースを有する複数の通信端末と、それらの通信端末を結ぶ通信網とを備えたグループ暗号通信システムであって、

前記ＩＣカードには、各ＩＣカードを特定する個別の数値、およびＩＣカードの所定の部分集合において共通であるマスタ鍵と呼ばれる秘密数値が複数個格納されているとともに、

前記ＩＣカードが差し込まれた端末は、通信を行うべき相手先を特定する通信宛先情報を生成し出力する手段と、自端末が生成しまたは外部端末が生成した通信宛先情報に基づいて自端末に差し込まれているＩＣカードに格納されている前記複数のマスタ鍵から１つを選択する手段と、選択したマスタ鍵を用いてグループ鍵を生成する手段と、生成したグループ鍵を用いて通信メッセージの暗号化および復合化を行う手段とを備えることを特徴とするグループ暗号通信システム。

【請求項９】前記通信宛先情報は、通信を行うべき相手先を特定する情報と任意に選択された数値情報とからなり、かつ前記グループ鍵を生成する手段は、前記選択したマスタ鍵および前記通信宛先情報を用いてグループ鍵を生成する請求項８に記載のグループ暗号通信システム。

【請求項１０】前記グループ鍵を生成する手段は、ハッシュ関数を用いた計算によってグループ鍵を生成する請求項８または９に記載のグループ暗号通信システム。

【請求項１１】前記ＩＣカードに格納されている個別の数値を用いて前記通信宛先情報を検査し、これにより該通信宛先情報が該ＩＣカードの個別の数値を指定しているか否かを判定する請求項８ないし１０に記載のグループ暗号通信システム。

【請求項１２】前記通信宛先情報に基づいて複数のマスタ鍵から１つを選択する手段と、選択したマスタ鍵を用いてグループ鍵を生成する手段とが、前記ＩＣカード内部に設けられている請求項８ないし１１に記載のグループ暗号通信システム。

【請求項１３】前記ＩＣカードにはさらに、暗号関数およびＩＣカードごとに異なる個別鍵と呼ばれる秘密数値

が格納されており、
該ＩＣカードは、マスタ鍵を個別鍵で暗号化したマスタ鍵暗号文を外部から入力し、該マスタ鍵暗号文を個別鍵と暗号関数を用いて復号化し、その結果を前記マスタ鍵が書かれていた記憶領域上に上書きすることにより、マスタ鍵の更新を行う手段を備えた請求項８ないし１２に記載のグループ暗号方法。
【請求項１４】前記ＩＣカードにはさらに、暗号関数およびＩＣカードごとに異なる第１，第２，…の個別鍵と呼ばれる秘密数値が複数個格納されており、
該ＩＣカードは、マスタ鍵を第１の個別鍵で暗号化したマスタ鍵分割暗号文を外部から入力し、マスタ鍵を第２の個別鍵で暗号化したマスタ鍵分割暗号文を外部からＩＣカードに入力し、…、このようにＩＣカードに入力された複数のマスタ鍵分割暗号文を前記第１，第２，…の個別鍵と暗号関数を用いてそれぞれ復号化し、その結果に所定の演算を施した結果を前記マスタ鍵が書かれていた記憶領域上に上書きすることにより、マスタ鍵の更新を行う手段を備えた請求項８ないし１２に記載のグループ暗号方法。
【発明の詳細な説明】
【０００１】
【産業上の利用分野】本発明は、通信メッセージを暗号化して送受する通信方法およびシステムに関する。
【０００２】
【従来の技術】近年、情報および通信の技術の進展によって、通信網を使って種々の情報を高速かつ安価にやりとりすることができるようになってきた。通信衛星やローカルエリアネットワークを使う場合、１つの情報を送信すると多数の端末で同時に受信することができる。すなわち、同報通信を簡単に実現できるという特徴がある。
【０００３】ところで、通信衛星やローカルエリアネットワークを使って同報通信を行う場合、送出された電気または電波信号はどの端末でも受信可能であり、そのままでは秘密にしたい情報を限定された相手にだけ伝えるような限定的通信を行うことはできない。
【０００４】通信衛星やローカルエリアネットワークを使って同報通信を行う場合に、限定された相手にだけ情報を伝え、それ以外の相手には情報を秘密にするための一方法が、例えば、宝木，福澤，中村，「カードによるセキュリティ」，情報社会における通信網の安全・信頼性シンポジウム，電子情報通信学会，１９９１年８月１９日などに示されている。
【０００５】図９を用いて、上記従来例で開示されている方法を説明する。
【０００６】図９は、従来の通信システムにおける受信側のワークステーション（ＷＳ）９０２、およびＩＣカード９０１を示している。
【０００７】先ず、ＷＳ９０２は通信網９１７経由で通信宛先情報を受け取る。通信宛先情報は、下記のような情報を含む。
【０００８】

通信宛先情報＝事業所番号１‖配布リスト１‖乱数１‖鍵情報１‖
事業所番号２‖配布リスト２‖乱数２‖鍵情報２‖
．
．
．

ここに、‖はデータのつなぎ合わせを示す。
【０００９】この後、ＷＳ９０２はＩＣカードのメモリ９０３から予め読み取っていた事業所識別番号９２５の数値「２」と個人識別番号９２６の数値「３」に基づいて、自ＷＳが通信宛先の対象に含まれているかどうかを検査する。例えば、上記の通信宛先情報のうち、事業所番号１が数値「２」であり、配布リスト１がビット列「００…０１０１」であったとする。この例では、ＷＳ９０２内のメモリ９１４に格納されている事業所識別番号９２５の数値は「２」で上記通信宛先情報の事業所番号１と一致している。また、ＷＳ９０２内のメモリ９１４に格納されている個人識別番号９２６の数値は「３」であるので、この数値「３」でポイントされる配布リスト１の下から３番目のビットを参照すると、それは「１」になっている。そこで、事業所識別番号９２５（数値は「２」）と個人識別番号９２６（数値は「３」）が該通信宛先情報に含まれている、と判定する。
【００１０】次に、ＷＳ９０２は、該当する通信宛先情報「事業所番号１‖配布リスト１‖乱数１‖鍵情報１」をＩＣカード９０１に送信する。そして、ＩＣカード９０１内でも、事業所識別番号９１８（数値は「２」）と個人識別番号９１９（数値は「３」）を使って同様の検査を行う。検査結果が「含まれている」であれば、単一事業所用マスタ鍵９２０を使って次の計算を行う。
【００１１】ワーク鍵←Ｈ(単一事業所用マスタ鍵，事業所番号１‖配布リスト１‖乱数１)
グループ鍵←Ｄ(ワーク鍵，鍵情報１)
ここに、Ｈ(Ｉ，Ｍ)は初期値をＩ、入力データをＭとするハッシュ関数Ｈによる出力（ハッシュトータル）である。また、Ｄ(Ｋ，Ｍ)は鍵をＫ、入力データをＭとする復号化関数Ｄによる出力である。
【００１２】ＩＣカード９０１は、以上のようにして算出したグループ鍵をＷＳ９０２に渡す。ＷＳ９０２は、このグループ鍵（メモリ９１４内のグループ鍵の記憶領域９２７に格納される）を使って、通信網９１７から送

信されてくる暗号メッセージを復号化する。

【００１３】以上により、ＩＣカード９０１が差し込まれているＷＳ９０２において、自ＷＳが通信宛先情報に含まれていることを判別し、鍵を生成して、暗号メッセージを復号化することができる。

【００１４】同様に他のＷＳにおいても、通信宛先情報に含まれる事業所識別番号と個人識別番号を持つＩＣカードが差し込まれていれば、グループ鍵を生成する処理が行われ、その結果通信網９１７から送信されてくる暗号メッセージを復号化できる状態となる。

【００１５】このようにして、１つの送信元から多数の受信先への一対多数の暗号通信を行うことができる。

【００１６】

【発明が解決しようとする課題】ところで、上記従来例において、一対多数通信のうちの多数の側の１つが送信側になることはできなかった。つまり、受信側のＩＣカードおよびＷＳが上記通信宛先情報を作成することはできなかった。これは、受信側のＩＣカードが該ＩＣカードが属する事業所にしか通用しない単一事業所用マスタ鍵を１つしか持たないためである。

【００１７】本発明の目的は、上述の従来例における問題点に鑑み、セキュリティ上の安全を確保しつつ、複数端末間で任意の１つの端末から任意の多数の端末へとグループ暗号通信ができるようにすることにある。

【００１８】

【課題を解決するための手段】上記課題を解決するため、本発明は、複数のＩＣカードと、ＩＣカードの入出力インターフェースを有する複数の通信端末と、それらの通信端末を結ぶ通信網とを備えた通信システムに適用するグループ暗号通信方法およびシステムであって、前記ＩＣカードには、各ＩＣカードを特定する個別の数値、およびＩＣカードの所定の部分集合において共通であるマスタ鍵と呼ばれる秘密数値が複数個格納されており、最初に通信を開始する端末においては、通信を行うべき相手先を特定する通信宛先情報を生成して、他の端末に送出するとともに、該通信宛先情報に基づいて自端末に差し込まれているＩＣカードに格納されている前記複数のマスタ鍵から１つを選択し、選択したマスタ鍵を用いてグループ鍵を生成し、生成したグループ鍵を用いて通信メッセージの暗号化および復合化を行って、通信メッセージを授受し、通信宛先である端末においては、前記通信宛先情報を受け取り、該通信宛先情報に基づいて自端末に差し込まれているＩＣカードに格納されている前記複数のマスタ鍵から１つを選択し、選択したマスタ鍵を用いてグループ鍵を生成し、生成したグループ鍵を用いて通信メッセージの暗号化および復合化を行って、通信メッセージを授受するようにしている。

【００１９】ＩＣカード毎の個別の数値は、ＩＣカードに入力される通信宛先情報と呼ばれるデータ列のある特定位置を検査するための、検査位置指定用のポインタとして用いるとよい。この検査によりそのＩＣカードが差し込まれた端末が通信宛先になっているのか否かが分かる。通信宛先になっているときは、通信宛先情報から複数のマスタ鍵のうちの１つを選択する。ＩＣカードのマスタ鍵は、この通信システム内の端末から正当にアクセスされたとき以外は読出すことができないようにしておくとよい。

【００２０】グループ鍵は、選択された秘密数値であるマスタ鍵と通信宛先情報を含むデータを入力としてハッシュ関数による計算を行って求めるとよい。

【００２１】さらにＩＣカードに、暗号関数とＩＣカード外部に出ないＩＣカードごとに異なる個別鍵と呼ばれる秘密数値を保持し、ＩＣカードに入力されるマスタ鍵暗号文と呼ばれるデータに対して、該個別鍵と暗号関数を用いて、復号化計算を行い、その計算結果を前記マスタ鍵が書かれていたエリア上に上書きすることにより、マスタ鍵の更新を行うようにしてもよい。

【００２２】

【作用】最初に通信を開始する端末は、通信を行うべき相手先を特定する通信宛先情報を生成して、他の端末に送出する。そして、通信宛先情報に基づいて自端末に差し込まれているＩＣカードに格納されている前記複数のマスタ鍵から１つを選択し、選択したマスタ鍵を用いてグループ鍵を生成し、生成したグループ鍵を用いて通信メッセージの暗号化および復合化を行って、通信メッセージを授受する。一方、通信宛先である端末は、前記通信宛先情報を受取り、該通信宛先情報に基づいて自端末に差し込まれているＩＣカードに格納されている前記複数のマスタ鍵から１つを選択し、選択したマスタ鍵を用いてグループ鍵を生成し、生成したグループ鍵を用いて通信メッセージの暗号化および復合化を行って、通信メッセージを授受する。結局、各端末において同一のマスタ鍵を用いてグループ鍵が生成される。したがって、複数事業所にまたがり好みの複数人の通信相手を指定して、グループ暗号通信を行うためのグループ鍵を共有することができる。

【００２３】通信中の事業所以外の事業所に属するＩＣカードの中身が万一漏洩したとしても、該事業所の間では特有のマスタ鍵が用いられるので、それらの事業所の間では通信の安全性に影響を与えることはない。複数事業所にまたがり鍵共有を行おうとする場合に、もし適当な部分域用マスタ鍵がＩＣカード内になかったときには、全域に有効なマスタ鍵を用いればよい。この場合、すべてのＩＣカードの中身が漏洩していなければ、安全である。

【００２４】上述の個別鍵を用いて暗号化したマスタ鍵暗号文を入力してマスタ鍵を更新する方式を用いれば、マスタ鍵漏洩等の事情によりマスタ鍵を更新する必要が生じた場合に、電話確認後個別暗号通信等の比較的安全な手段によりマスタ鍵を更新することが可能になる。

【００２５】また、複数の個別鍵を用いて暗号化したマスタ鍵分割暗号文を入力してマスタ鍵を更新する方式では、マスタ鍵が複数の鍵センタの共同作業により生成されることになる。したがって、複数の鍵センタが結託しない限り、マスタ鍵が鍵センタの単独作業により知られることはない。よって、通信当事者間のプライバシーを鍵センタに対しても保護することができる。

【００２６】

【実施例】以下、図面を用いて、本発明の実施例を説明する。

【００２７】図１０は、本発明のグループ暗号方法および装置を適用した暗号通信システムを示す。この暗号通信システムは、ＩＣカードの入出力インターフェースを有する５つの通信端末１００２，１００４，１００６，１００８，１０１０、およびそれらを結ぶ通信網１００１を備えている。通信端末１００２，１００４，1006，１００８，１０１０には、それぞれＩＣカード１００３，１００５，１００７，１００９，１０１１が差し込まれている。

【００２８】各ＩＣカードには、ＩＣカード別の個別の数値１０１２，１０１６，１０１９，１０２３，１０２６が記憶されている。この個別数値（ｘ，ｙ）の、ｘは事業所番号、ｙはその事業所内の個人番号を示す。ここでは事業所番号「１」が本社、「２」がＡ事業所を表すものとする。ＩＣカード１００３の個別数値１０１２は（１，１）であるからこのカードは本社のａさん用、ＩＣカード１００５の個別数値１０１６は（１，２）であるからこのカードは本社のｂさん用、ＩＣカード１００７の個別数値１０１９は（２，１）であるからこのカードはＡ事業所のｃさん用、ＩＣカード１００９の個別数値１０２３は（２，２）であるからこのカードはＡ事業所のｄさん用、ＩＣカード１０１１の個別数値１０２６は（２，３）であるからこのカードはＡ事業所のｅさん用、というようになる。

【００２９】さらに、各ＩＣカードには、ＩＣカードから外部への読出しが禁止されているマスタ鍵と呼ばれる秘密数値が格納されている。このうち、本社用マスタ鍵1013，１０１７は、本社のａさん用カード１００３とｂさん用カード１００５で共通である。また、Ａ事業所用マスタ鍵１０２０，１０２４，１０２７は、Ａ事業所のｃさん用カード１００７、ｄさん用カード１００９およびｅさん用カード1011で共通である。全域用マスタ鍵１０１５，１０１８，１０２２，１０２５，1029は、５枚のＩＣカード１００３，１００５，１００７，１００９，１０１１すべてで共通である。

【００３０】図１は、図１０のうちＡ事業所のｅさん用カード１０１１と通信端末１０１０の詳細を示す。図１において、ＩＣカード１０１（図１０の１０１１）は、ＩＣカード側インターフェース１０５およびＷＳ側インターフェース１０９を経由して、ワークステーション（ＷＳ）１０２とデータのやりとりを行う。ＷＳ１０２は、通信ボード１０８を経由して通信網１１７とデータのやりとりを行う。

【００３１】ＩＣカード１０１では、メモリ１０４内のグループ鍵生成プログラム１にしたがってＣＰＵ１０６が動作する。メモリ１０３内の事業所識別番号１１８（図１０の個別数値１０２６の第１番目）の数値は「２」で、個人識別番号１１９（図１０の個別数値１０２６の第２番目）の数値は「３」が格納されており、該ＩＣカード１０１の所有者は事業所番号「２」の事業所（Ａ事業所）に属する番号「３」の個人であることを示す。より具体的には、メモリ１１３に格納されている識別番号ー識別名対応表１２４により、該ＩＣカード１０１の所有者はＡ事業所のＥさんであることが分かる。単一事業所用マスタ鍵１２０（図１０の1017），全域用マスタ鍵１２１（図１０の１０２９），部分域用マスタ鍵１２２，１２３（図１０の１０２８），…はそれぞれ６４ビット長のランダムなデータである。

【００３２】ＷＳ１０２では、メモリ１１５内のグループ鍵生成プログラム２にしたがってＣＰＵ１１０が動作する。メモリ１１３内の識別番号ー識別名対応表１２４は、事業所番号「１」は本社であることを示し、本社内の個人番号「１」はａさん、個人番号「２」はｂさん、…であることを示す。同様に、事業所番号「２」はＡ事業所であることを示し、Ａ事業所内の個人番号「１」はｃさん、個人番号「２」はｄさん、個人番号「３」はｅさん、…であることを示す。メモリ１１４は、このＷＳ１０２に差し込まれたＩＣカード１０１の事業所識別番号１１８および個人識別番号１１９を読出して格納する領域１２５，１２６を有する。ここでは事業所識別番号１１８が「２」、個人識別番号１１９が「３」であるので、事業所識別番号１２５は「２」、個人識別番号１２６は「３」になっている。また、メモリ１１４は、グループ鍵の生成結果を格納する領域１２７を有する。

【００３３】その他、ＷＳ１０２には、ＷＳの操作員に入出力手段を提供するディスプレイ１１１、およびキーボード１１２などを備えている。

【００３４】上述したように、各ＩＣカードはその所有者に固有の事業所識別番号および個人識別番号（図１０では個別数値と呼んでいる）を格納している。ＩＣカードを通信網１１７内のいずれかの端末に差し込むことにより、その所有者は通信網１１７を介して他の人と通信し合える環境となる。

【００３５】以下、通信網の誰かが複数の通信相手を任意に指定して暗号通信を行おうとする場合に、それらの通信相手と暗号鍵を共有し合う方式について説明する。

【００３６】図２は、メモリ１１５に格納されているグループ鍵生成プログラム２の動作を説明するためのフローチャートである。まずステップ２０１で処理が開始され、ステップ２０２で、操作員はキーボード１１２より

最初に鍵生成を行うことを示すコマンド、もしくは他の通信相手の後で鍵生成を行うことを示すコマンドを入力する。ステップ２０３では、もし前者のコマンドであればステップ２０４へ、もし後者のコマンドであればステップ２１１へ、それぞれ分岐する。最初に鍵生成を行うということは、この端末から他の端末に向けて最初に通信を開始するということであり、そのために最初に鍵生成を行う。他の通信相手の後で鍵生成を行うということは、他の通信相手が最初に鍵生成を行って通信を開始しており、その通信相手からのメッセージなどを受け取るために鍵生成を行うということである。

【００３７】最初に鍵生成を行うときは、まずステップ２０４でディスプレイ１１１へ識別番号ー識別名対応表１２４を表示する。次に、ステップ２０５で、操作員は該ディスプレイ１１１の表示を見て通信相手を選び、キーボード１１２より通信相手と自分の所属および名前を入力する。ここでは、操作員がＡ事業所のｅさんであるものとし、ｅさんが本社のａさんおよびＡ事業所のｃさんを通信相手に選び、それらの事業所識別番号と個人識別番号を入力したとする。さらに、自分の所属と名前であるＡ事業所のｅを特定する事業所識別番号と個人識別番号も入力する。

【００３８】次に、ステップ２０６で、該入力情報と識別番号ー識別名対応表１２４を参照して、図４に示すような通信宛先情報を生成する。通信宛先情報は、事業所番号と配布リストを並べたものと乱数とからなる。事業所番号は２進の数値データ、配布リストは各ビットがその事業所の各個人に対応しているビットデータである。

【００３９】図４において、事業所番号（事業所識別番号）４０１は２進数の数値データ「１」であることにより、事業所番号が「１」、すなわち本社が通信宛先の１つであることを示す。配布リスト４０２は、ビット列の下から第２ビット目がビット「１」であることにより、本社(事業所番号が「１」）の個人識別番号が「２」、すなわちａさんが通信宛先の１人であることを示す。同様に、事業所番号403は値「２」でＡ事業所が通信宛先の１つであり、その配布リスト４０４は個人識別番号が「１」と「３」、すなわちｃさんとｅさんがそれぞれ通信宛先の１人であることを示す。また、乱数４０５は本ステップ２０６の実施時点で新たに生成される乱数である。このような通信宛先情報を生成して、ＩＣカード１０１に送信する。

【００４０】次に、ステップ２０７でＩＣカード１０１において図３に示す動作（後述するグループ鍵の生成）が実施される。その間、ＷＳ１０２側は待機する。ＩＣカード１０１でのグループ鍵の生成が終了したら、ステップ２０８でＩＣカード101から返される値であるグループ鍵を受け取り、メモリ１１４内のグループ鍵の記憶領域１２７に書き込む。そして、ステップ２０９で該通信宛先情報（図４）を通信ボード１０８経由で通信網１１７に送信し、ステップ２１０で処理を終了する。以後、この端末では生成したグループ鍵を用いて通信メッセージを暗号化し送出する。また、相手から送られてきた通信メッセージは生成したグループ鍵を用いて解読する。

【００４１】次に、最初に鍵を生成するのではないときは、まずステップ２１１でＩＣカード１０１内のデータである事業所識別番号１１８と個人識別番号１１９をＷＳ１０２内のメモリ１１４の領域１２５と１２６に書き込む。次に、ステップ212で通信網１１７から通信宛先情報が来るのを待機する。通信宛先情報が来たら次のステップへ進む。本例では、図４の通信宛先情報を受信するものとする。

【００４２】ステップ２１３では、該通信宛先情報がメモリ１１４の事業所識別番号１２５と個人識別番号１２６で示される宛先を含んでいるかどうかを検査する。もし、含んでいればステップ２１４に進み、さもなければステップ２１８へ進み処理を終了する。

【００４３】ステップ２１４では、該通信宛先情報をＩＣカード１０１に送信する。そして、ステップ２１５でＩＣカード１０１において図３に示す動作（後述するグループ鍵の生成）が実施される。その間、ＷＳ１０２側は待機する。ＩＣカード101でのグループ鍵の生成が終了したら、ステップ２１６でＩＣカード１０１から返される値であるグループ鍵を受け取り、メモリ１１４内のグループ鍵の記憶領域１２７に書き込む。そして、ステップ２１７で処理を終了する。以後、この端末では生成したグループ鍵を用いて、受け取った通信メッセージを解読する。また、相手に通信メッセージを送るときは、生成したグループ鍵を用いて暗号化し送出する。

【００４４】図３は、メモリ１０４に格納されているグループ鍵生成プログラム１の動作を説明するためのフローチャートを示す。まずステップ３０１で処理が開始され、ステップ３０２でＩＣカード側インターフェース１０５経由で通信宛先情報（図４）を受信する。次に、ステップ３０３で該通信宛先情報に事業所識別番号118と個人識別番号１１９が同時に含まれるかどうかを検査する。もし、含まれていればステップ３０４へ進む。さもなければ、ステップ３０８へ進む。

【００４５】いま図３の処理が実行されているＩＣカードが図１のＩＣカード１０１（Ａ事業所のｅさんのもの）であって、受け取った通信宛先情報が図４に示す数値例の場合は、事業所番号４０３の欄が数値「２」で、それに引き続く配布リスト404の欄で第３ビット目にビット「１」が立っていることから、事業所識別番号118（数値は「２」）と個人識別番号１１９（数値は「３」）が同時に含まれていると判定される。

【００４６】次に、ステップ３０４では、使用すべきマスタ鍵の種類を図６に示す手順（後述する）で選定する。そして、ステップ３０５で該宛先通信情報と該マス

タ鍵を使ってハッシュトータルを計算する。すなわち、
ハッシュトータル←H（マスタ鍵，宛先通信情報）
とする。ここに、H(K，M)はハッシュ関数であり、例えば、文献：宝木，「暗号方式と応用」，情報処理学会誌，１９９１年６月、で定義されたものなどを用いる。次に、ステップ３０６で該ハッシュトータルをＩＣカード側インターフェース１０５経由でＷＳ１０２に出力し、ステップ３０７で処理を終了する。このハッシュトータルがグループ鍵として用いられる。

【００４７】一方、ステップ３０３で通信宛先情報に事業所識別番号１１８と個人識別番号１１９が同時に含まれていないときは、ステップ３０８で「拒否」通知をＩＣカード側インターフェース１０５経由でＷＳ１０２に出力し、ステップ３０９で処理を終了する。

【００４８】図６は、図３の処理のうちのステップ３０４の詳細な動作を説明するためのフローチャートを示す。まず、ステップ６０１で処理が開始されると、ステップ６０２で通信宛先情報(図４)内の事業所番号のデータが１つだけかどうかを検査する。もし、１つだけならその事業所のみとの通信であるから、ステップ６０８へ進み、単一事業所用マスタ鍵１２０をメインルーチンへ返して、ステップ609へ進む。ステップ６０２で通信宛先情報（図４）内の事業所番号のデータが１つより多いときは、ステップ６０３へ進む。図４の数値例では事業所番号欄の数は２つ以上ある。

【００４９】次に、ステップ６０３でメモリ１０３に記録されている部分域用マスタ鍵122，１２３，…がすべて検査されたかどうかを判定する。もし、すべて検査されたのであれば、ステップ６０７へ進む。さもなければ、ステップ６０４へ進む。図５は、部分域用マスタ鍵のフォーマット例を示す。部分域用マスタ鍵は、事業所リスト５０１とそれに対するマスタ鍵情報５０２を備えている。事業所リスト501は、各事業所に対応するビットを並べたビットデータである。図５の例では、事業所リスト５０１の最下位ビット（第１ビット）が「１」、第２ビットが「１」で、他のビットは「０」であるから、このマスタ鍵情報５０２は事業所識別番号が「１」および「２」の事業所のグループの部分域用マスタ鍵であることとなる。

【００５０】次に、ステップ６０４では、該部分域用マスタ鍵(図５)の事業所リスト５０１の欄が該通信宛先情報（図４）に示される事業所をすべて含むかどうかを検査する。もし、含まれていれば、ステップ６０６に進む。さもなければ、ステップ６０５に進む。図５の数値例では、事業所リスト５０１は事業所識別番号が「１」と「２」である。図４の数値例では事業所番号４０１は事業所「１」を、事業所番号４０３は事業所「２」を示している。図４においてその他の…の部分が空白であれば、部分域用マスタ鍵（図５）の事業所リスト（５０１）の欄は該通信宛先情報（図４）に示される事業所をすべて含むことになる。

【００５１】ステップ６０４で部分域用マスタ鍵の事業所リスト５０１の欄が通信宛先情報に示される事業所をすべて含むのでない場合は、ステップ６０５でメモリ１０３上の次の部分域用マスタ鍵を設定する。そして、ステップ６０３へ戻る。

【００５２】ステップ６０４で部分域用マスタ鍵の事業所リスト５０１の欄が通信宛先情報に示される事業所をすべて含む場合は、ステップ６０６で該部分域用マスタ鍵（図１の部分域用マスタ鍵１２２，１２３，…のうちの１つ）をメインルーチンへ渡す。そして、ステップ６０９へ進む。

【００５３】ステップ６０３で部分域用マスタ鍵をすべて調べた場合は、ステップ６０７で全域用マスタ鍵１２１をメインルーチンへ渡す。そして、ステップ６０９へ進む。ステップ６０９で処理を終了する。

【００５４】上述したように、単一事業所用マスタ鍵１２０は、同じ事業所に属するＩＣカードではすべて同じ値が書かれている。例えば、Ａ事業所のｃさん，ｄさん、およびｅさんのＩＣカードの単一事業所用マスタ鍵１２０はすべて同じ値である。また、全域用マスタ鍵１２１は、事業所が同じかどうかにかかわらずすべてのＩＣカードで同じ値である。部分域用マスタ鍵１２２，１２３…は、事業所リスト（図５の５０１）で指定される事業所に属すＩＣカードはすべて同じ値である。例えば、図５の５０１の例は、事業所番号「１」と「２」すなわち、本社とＡ事業所に属するＩＣカードに記録されるものである。

【００５５】以上より、本実施例によれば、ディスプレイ１１２に表示される事業所別識別名一覧表１２４を見て通信相手を選定しキーボードを入力することにより、ＩＣカード１０１で自分および通信相手に共通に保持されるグループ鍵が生成され、ＷＳ１０２のメモリ１１４にそのグループ鍵が設定される。つまり、複数事業所にまたがり好みの複数人の通信相手を指定して、グループ暗号通信を行うためのグループ鍵を共有することができる。

【００５６】また、グループ鍵を計算するうえで、
グループ鍵←H（マスタ鍵，通信宛先情報）　（ただし、Hはハッシュ関数）
の計算式で使用されるマスタ鍵は、ＩＣカード１０１に入力される通信宛先情報（図４）の数値データによって異なる。例えば、図４に記入された数値例の場合、もし図の…の部分が空白であれば、図５の数値例に示されるような部分域用マスタ鍵が使用される。この部分域用マスタ鍵は、事業所番号「１」と「２」、すなわち本社とＡ事業所に属するＩＣカードにしか入っていない数値データである。これにより、他の事業所に属するＩＣカードの中身が万一漏洩したとしても本マスタ鍵は含まれないので、本事業所番号「１」と「２」の間の通信の安全

性に影響を与えることはない。

【００５７】複数事業所にまたがり鍵共有を行おうとする場合に、もし適当な部分域用マスタ鍵がＩＣカード内になかったとする。このときは、全域用マスタ鍵が使われ、グループ鍵が生成される。各ＩＣカードには、全域用マスタ鍵のほかに単一事業所用マスタ鍵や幾つかの部分域用マスタ鍵が含まれている。したがって、例えば１枚のＩＣカードの中身が漏洩したとすると全域用マスタ鍵が知られてしまうので、その場合の安全性は低下するが、すべてのＩＣカードの中身が漏洩していない限り、グループ間の通信においては安全性が高い。指定された通信相手のＩＣカード以外ではグループ鍵は生成されないからである。

【００５８】（実施例の変形例１）前記の実施例では、ＩＣカード１０１内のマスタ鍵１２０，１２１，１２２，１２３，…は、予め設定されているとした。この代わり、図７に示すように、ＩＣカード１０１内のメモリ１０３に予めＩＣカード個別の個人鍵７０１を設定しておき、各個人鍵を集中管理する鍵センタからマスタ鍵１２０，１２１，122,１２３，…をＩＣカード別に個人鍵７０１で暗号化しマスタ鍵暗号文として送信し、受信側のＩＣカード内の暗号関数７０２でそのマスタ鍵暗号文を復号化してメモリ１０３内に設定するようにしてもよい。

【００５９】この変形例１により、マスタ鍵漏洩等の事情でマスタ鍵を更新する必要が生じた場合に、電話確認後個別暗号通信等の比較的安全な手段によりマスタ鍵を更新することが可能になる。

【００６０】（実施例の変形例２）前記の実施例では、ＩＣカード１０１内のマスタ鍵１２０，１２１，１２２，１２３，…は、予め設定されているとした。この代わり、図８に示すように予めＩＣカード個別に第１のセンタに登録されている個人鍵８０１、第２のセンタに登録されている個人鍵８０２、…を設定しておく。各センタは、ＩＣカードの鍵を集中管理する。マスタ鍵更新時には、第１のセンタから、マスタ鍵情報を生成するために用いる第１のマスタ鍵登録情報を個人鍵８０１で暗号化しマスタ鍵分割暗号文として送信する。受信側のＩＣカードでは、暗号関数７０２でこのマスタ鍵分割暗号文を復号化し、第１のマスタ鍵登録情報を得る。同様に、第２のセンタから、第２のマスタ鍵登録情報を個人鍵８０２で暗号化して送信し、受信側のＩＣカード内の暗号関数７０２で復号化し、第２のマスタ鍵登録情報を得る。他のセンタがある場合は、同様にしてマスタ鍵登録情報を得る。そして、ＩＣカード１０１内で、

マスタ鍵←第１のマスタ鍵登録情報＋第２のマスタ鍵登録情報＋…

（ただし「＋」はビット毎の排他的論理和とする）の計算式でマスタ鍵を計算して、メモリ１０３内に設定するようにしてもよい。

【００６１】この変形例２によれば、マスタ鍵は複数の鍵センタの共同作業により生成される。したがって、複数の鍵センタが結託しない限り、マスタ鍵がセンタに知られることはない。

【００６２】（実施例の変形例３）前記の実施例では、図４に示すように通信宛先情報の最後の欄４０５を乱数としていたが、乱数ではなく時間の経過とともに異なるような時間情報やシーケンス番号等にしてもよい。

【００６３】

【発明の効果】以上説明したように、本発明によれば、複数事業所にまたがり好みの複数人の通信相手を指定して、グループ暗号通信を行うためのグループ鍵を共有することができる。また、通信中の事業所以外の事業所に属するＩＣカードの中身が万一漏洩したとしても、該事業所の間の通信の安全性に影響を与えることはない。

【００６４】さらに、複数事業所にまたがり鍵共有を行おうとする場合、もし適当な部分域用マスタ鍵がＩＣカード内になかったときには、全域用マスタ鍵が使われ、グループ鍵が生成される。この場合でも、すべてのＩＣカードの中身が漏洩していなければ、安全である。

【００６５】個人鍵などを用いれば、マスタ鍵漏洩等の事情によりマスタ鍵を更新する必要が生じた場合に、電話確認後個別暗号通信等の比較的安全な手段によりマスタ鍵を更新することが可能になる。さらに、マスタ鍵が複数の鍵センタの共同作業により生成されるようにして、複数の鍵センタが結託しない限りマスタ鍵が鍵センタの単独作業により知られることがないようにできる。したがって、通信当事者間のプライバシーを鍵センタに対して保護することができる。

【図面の簡単な説明】

【図１】本発明の第１の実施例である通信システムにおける端末の構成図を示す。

【図２】図１におけるグループ鍵生成プログラム２の動作フローチャートを示す。

【図３】図１におけるグループ鍵生成プログラム１の動作フローチャートを示す。

【図４】図１におけるＩＣカード１０１に入力される通信宛先情報のフォーマット、および数値データ例を示す図である。

【図５】図１における部分域用マスタ鍵１２２，１２３，…のフォーマット、および数値データ例を示す図である。

【図６】図３の処理のうちのステップ３０４の詳細な動作フローチャートを示す。

【図７】実施例の変形例１のシステム構成図を示す。

【図８】実施例の変形例２のシステム構成図を示す。

【図９】従来例のシステム構成図を示す。

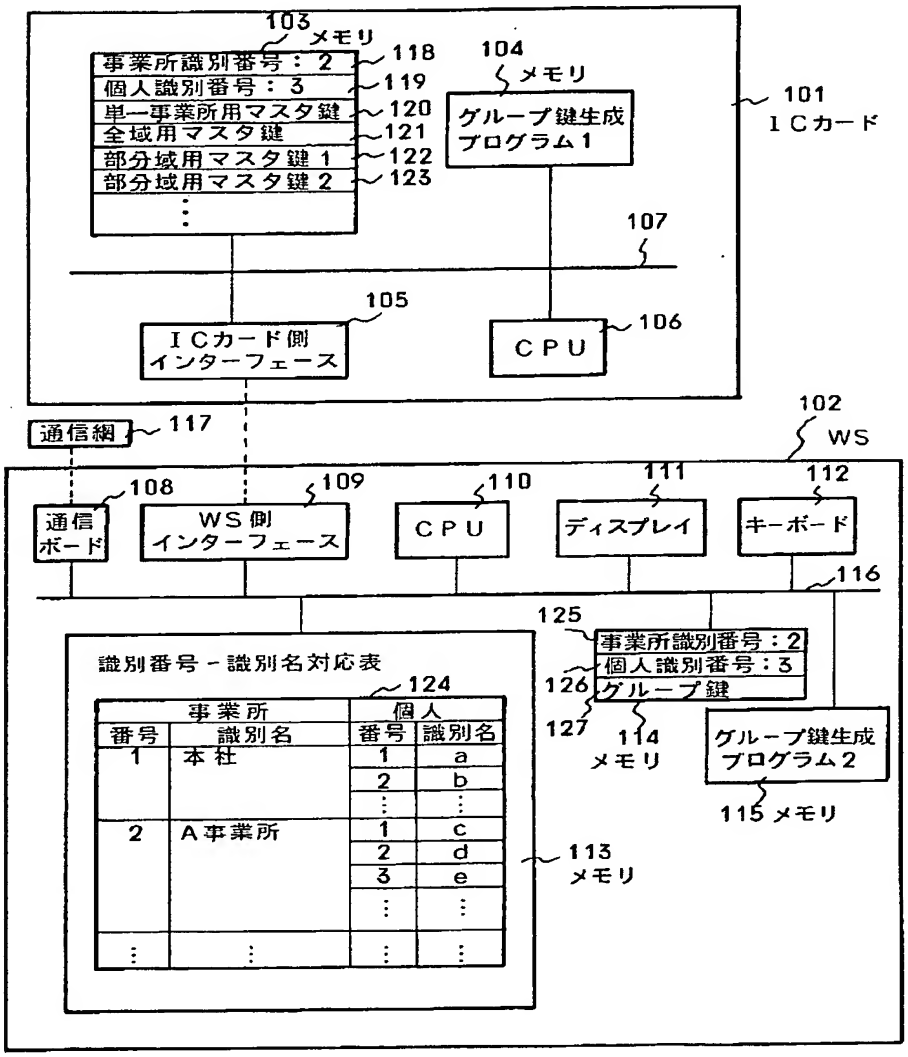
【図１０】本発明の第１の実施例である通信システムの構成図を示す。

【符号の説明】

１００１…通信網、１００２，１００４，１００６，１００８，１０１０…通信端末、１００３，１００５，１００７，１００９，１０１１…ＩＣカード、１０１２，１０１６，１０１９，１０２３，１０２６…個別数値、１０１３，１０１７…本社用マスタ鍵、１０２０，１０２４，１０２７…Ａ事業所用マスタ鍵、１０１５，１０１８，１０２２，１０２５，１０２９…全域用マスタ鍵、１０１…ＩＣカード、１０２…ワークステーション（ＷＳ）、１０３，１０４，１１３，１１４，１１５…メモリ、１０６，１１０…ＣＰＵ、１１７…通信網。

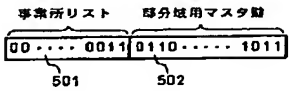
【図１】

図 1



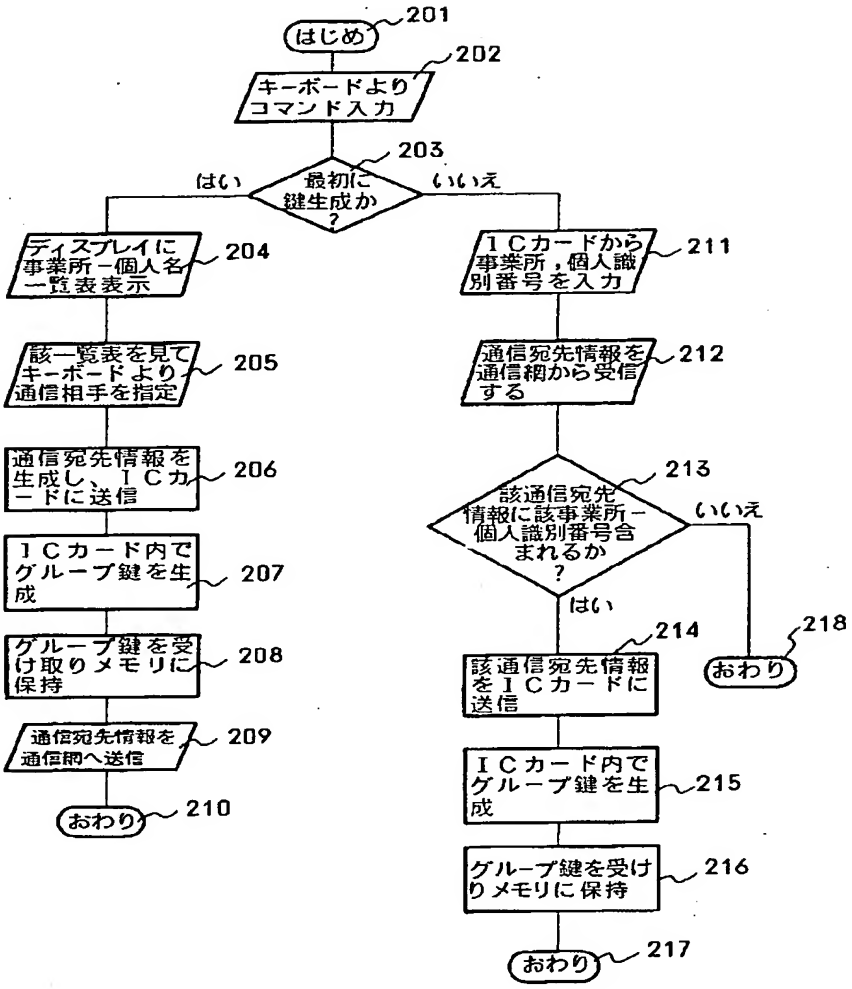
【図５】

図 5



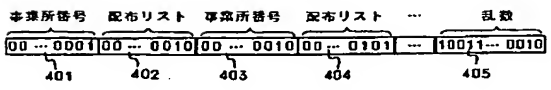
【図２】

図　２


はじめ
201
キーボードよりコマンド入力
202
最初に鍵生成か？
203
はい
いいえ
ディスプレイに事業所－個人名一覧表表示
204
該一覧表を見てキーボードより通信相手を指定
205
通信宛先情報を生成し、ＩＣカードに送信
206
ＩＣカード内でグループ鍵を生成
207
グループ鍵を受け取りメモリに保持
208
通信宛先情報を通信網へ送信
209
おわり
210
ＩＣカードから事業所，個人識別番号を入力
211
通信宛先情報を通信網から受信する
212
該通信宛先情報に該事業所－個人識別番号含まれるか？
213
いいえ
はい
該通信宛先情報をＩＣカードに送信
214
おわり
218
ＩＣカード内でグループ鍵を生成
215
グループ鍵を受けりメモリに保持
216
おわり
217

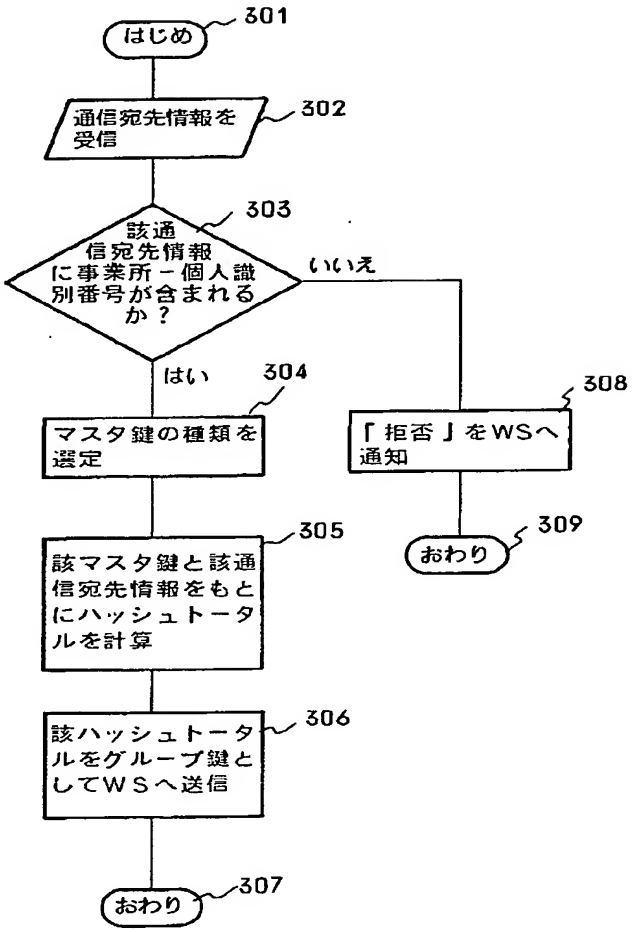
【図４】

図　４


事業所番号
配布リスト
事業所番号
配布リスト
…
乱数
00 … 0001
00 … 0010
00 … 0010
00 … 0101
…
10011… 0010
401
402
403
404
405

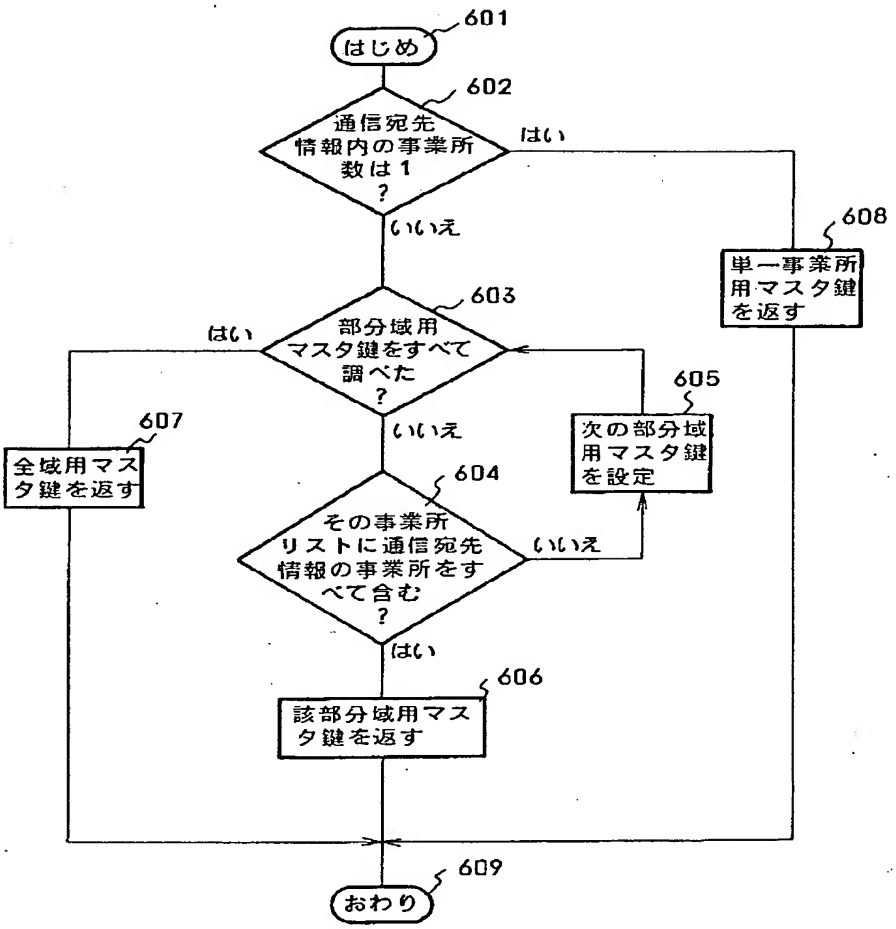
【図３】

図 ３



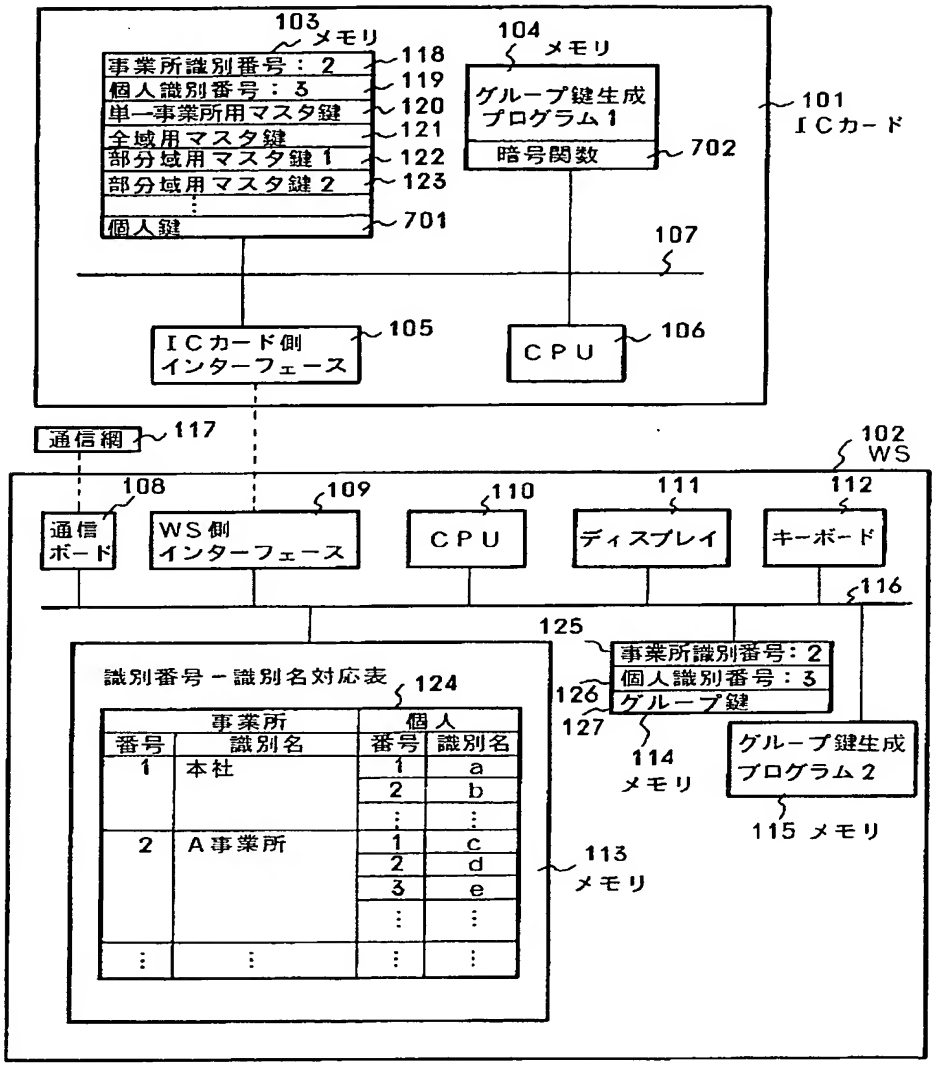
【図６】

図 ６


601
はじめ
602
通信宛先情報内の事業所数は１？
はい
いいえ
608
単一事業所用マスタ鍵を返す
603
部分域用マスタ鍵をすべて調べた？
はい
いいえ
605
次の部分域用マスタ鍵を設定
607
全域用マスタ鍵を返す
604
その事業所リストに通信宛先情報の事業所をすべて含む？
いいえ
はい
606
該部分域用マスタ鍵を返す
609
おわり

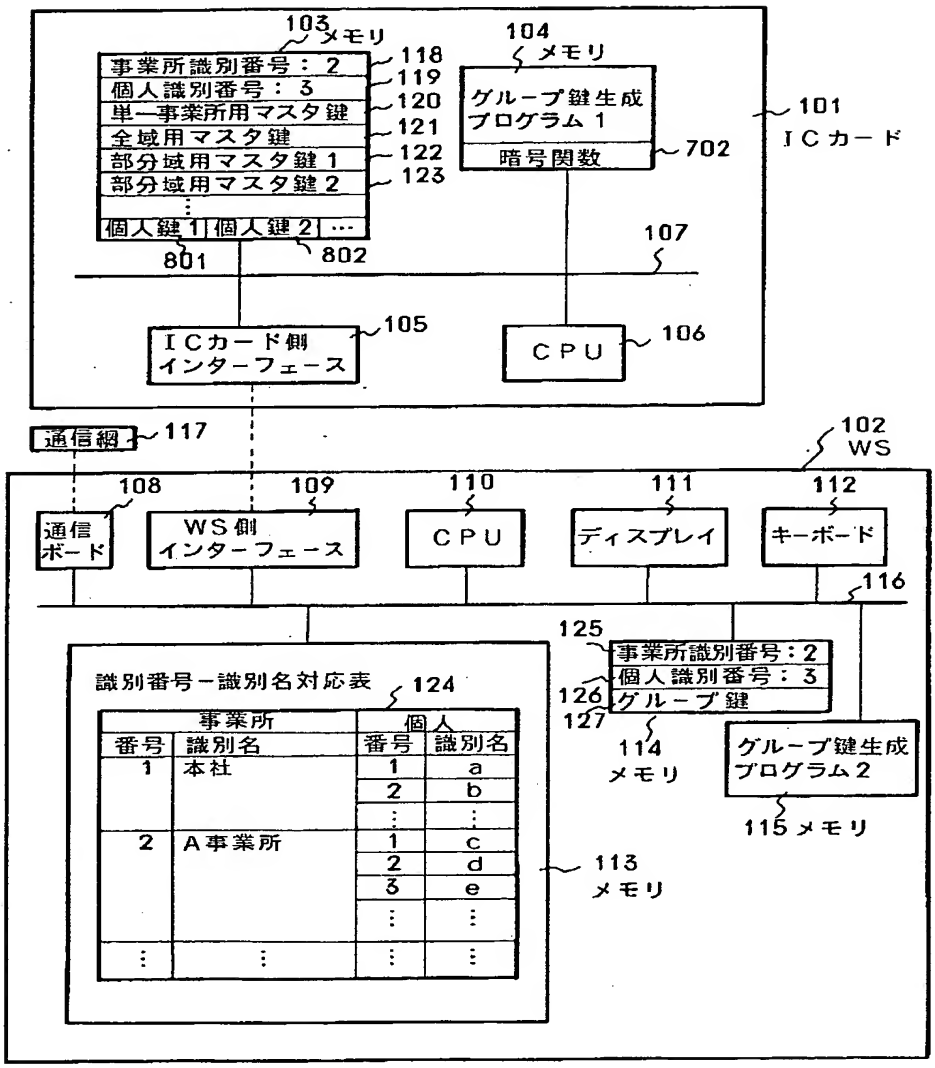
【図７】

図 ７


103
メモリ
事業所識別番号：２
個人識別番号：３
単一事業所用マスタ鍵
全域用マスタ鍵
部分域用マスタ鍵１
部分域用マスタ鍵２
個人鍵
118
119
120
121
122
123
701
104
メモリ
グループ鍵生成プログラム１
暗号関数
702
101
ＩＣカード
107
ＩＣカード側インターフェース
105
ＣＰＵ
106
通信網
117
102
WS
108
通信ボード
109
WS側インターフェース
110
ＣＰＵ
111
ディスプレイ
112
キーボード
116
125
事業所識別番号：２
個人識別番号：３
126
グループ鍵
127
114
メモリ
グループ鍵生成プログラム２
115 メモリ
識別番号－識別名対応表
124
事業所
個人
番号
識別名
1
本社
2
A事業所
a
b
c
d
e
113
メモリ

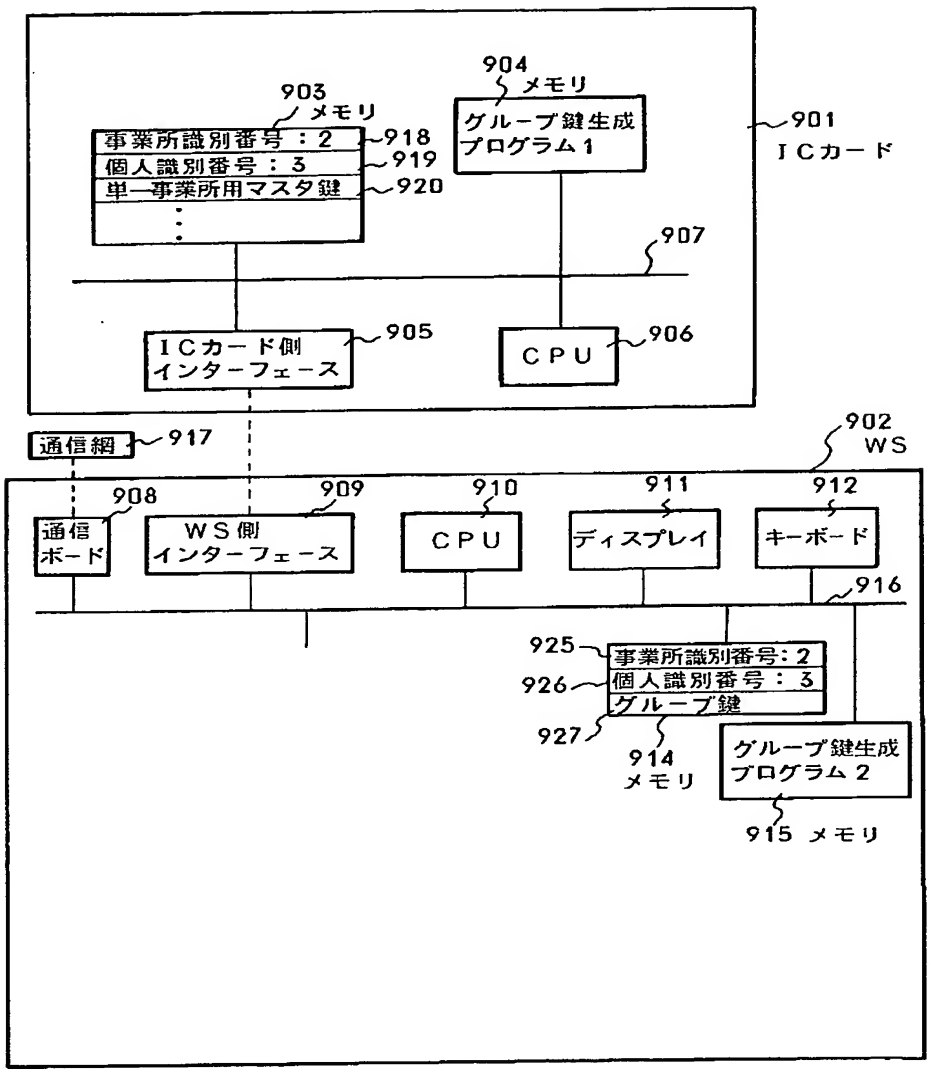
【図８】

図 ８


103 メモリ
事業所識別番号：２
個人識別番号：３
単一事業所用マスタ鍵
全域用マスタ鍵
部分域用マスタ鍵１
部分域用マスタ鍵２
個人鍵１ 個人鍵２ …
118
119
120
121
122
123
801
802
104 メモリ
グループ鍵生成プログラム１
暗号関数
702
101 ＩＣカード
107
ＩＣカード側インターフェース
105
ＣＰＵ
106
通信網
117
102 WS
108 通信ボード
109 WS側インターフェース
110 ＣＰＵ
111 ディスプレイ
112 キーボード
116
125
事業所識別番号：２
個人識別番号：３
グループ鍵
126
127
114 メモリ
グループ鍵生成プログラム２
115 メモリ
識別番号－識別名対応表
124
事業所
番号 識別名
1 本社
2 A事業所
個人
番号 識別名
1 a
2 b
1 c
2 d
3 e
113 メモリ

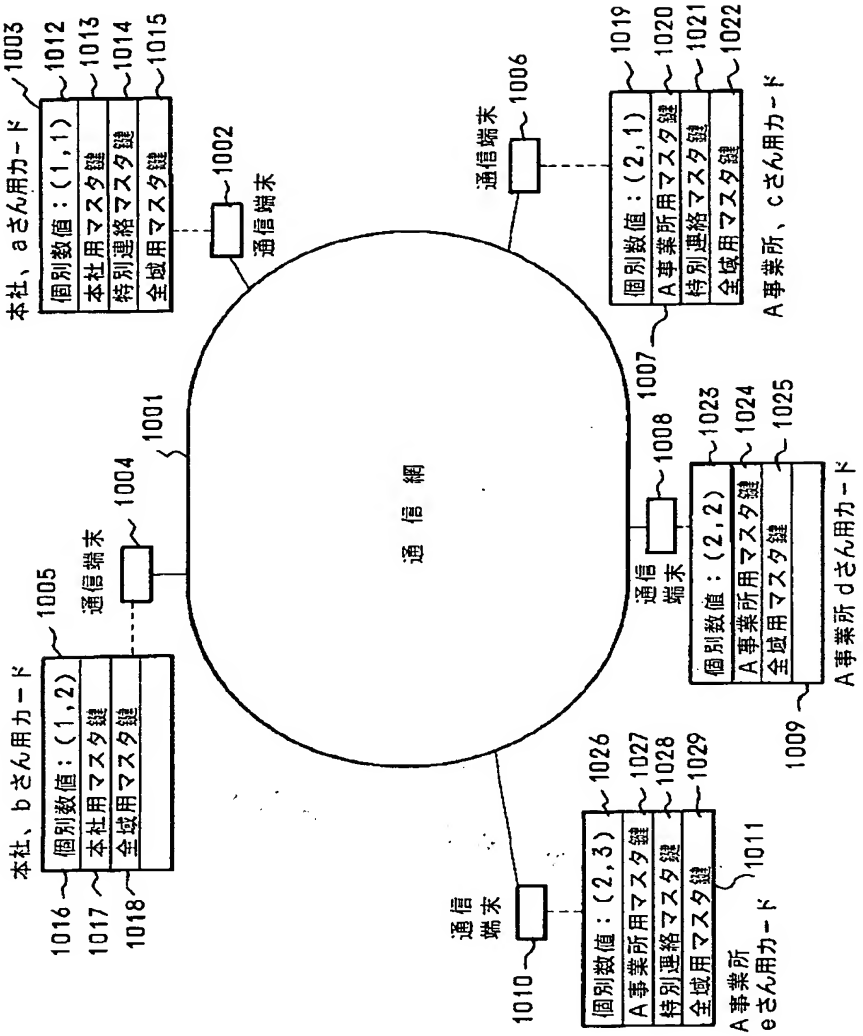
【図９】

図 ９


903
メモリ
事業所識別番号：2
個人識別番号：3
単一事業所用マスタ鍵
918
919
920
904
メモリ
グループ鍵生成
プログラム１
901
ＩＣカード
907
ＩＣカード側
インターフェース
905
ＣＰＵ
906
通信網
917
902
WS
908
通信
ボード
909
ＷＳ側
インターフェース
910
ＣＰＵ
911
ディスプレイ
912
キーボード
916
925
事業所識別番号：2
926
個人識別番号：3
グループ鍵
927
914
メモリ
グループ鍵生成
プログラム２
915
メモリ

【図１０】

図 １０



フロントページの続き

(72)発明者　松本　浩
愛知県名古屋市中区栄三丁目10番22号　日　45立中部ソフトウエア株式会社内

(72)発明者　中村　勤
神奈川県川崎市麻生区王禅寺1099番地　株式会社日立製作所システム開発研究所内